

ABSTRACT OF THE DISCLOSURE

A method and apparatus to provide pre-boot security and legacy hardware and environment support for a computing system having an extensible firmware architecture is described. A virtual machine monitor is employed to provide the virtualization of system state for the purposes of running legacy compatibility code or protecting key data and code regions for safety and security. An application may be given access to a subset of the system resources, and access to portions of the memory map not designated for updates would trap (program interrupt) to the VMM. A VMM pre-boot policy agent may then protect state and unload any problematic software.

09604-0974
T04250 "5T099650